

信息时代下的网络安全管理

呼博文

中国电信集团有限公司 北京 100010

摘要: 随着当前我国互联网技术的不断发展, 人民群众越来越离不开信息网络。然而, 信息时代下的网络发展虽然给人们带来了极大的便利, 但是也存在着一一定的危险性, 从而影响着人们的信息安全和财产安全。本文主要对信息时代下的网络安全管理进行探究, 提出一些策略, 从而更好的保障网络安全工作的开展。

关键词: 信息时代; 网络安全; 安全管理

Network security management in the Information age

Bowen Hu

China Telecom Group Co., Ltd. (Beijing) 100010

Abstract: With the continuous development of Internet technology in our country, the masses are more and more inseparable from the information network. However, although the development of the network in the information age has brought great convenience to people, it also has certain dangers, which affect people's information security and property security. This paper mainly explores network security management in the information age and puts forward some strategies to better ensure the development of network security work.

Key words: information age; Network security; security management

前言

在当前随着我国经济社会的不断发展以及进步, 信息技术在我国也得到了大范围的运用, 并且我们也进入了 5G 时代, 信息时代下无论是大数据还是云技术的发展, 都为各行各业带来了极大的便利。同时, 用户通过网络搜索能够了解到自己想了解的内容和知识。互联网技术的不断发展, 促进了一些新的行业出现。例如, 自媒体以及跨境电商和电子商务等, 这些行业的出现, 解决了许多就业难的问题, 这也为企业的发展带来了新的时机。并且, 伴随着互联网技术在各行各业的运用, 个人的信息也能够参与到医疗, 社交等多个平台上面。然而, 信息时代在为人们带来极大便利的过程中, 也使得个人的信息遭到了泄露。正因为个人信息在各个平台上的使用, 这就为一些不法分子提供了便捷。在信息时代背景下网络安全管理也是非常重要的, 这些不法分子, 他们会利用用户的信息来做一些违法乱纪的事情, 而且如果用户个人信息遭到泄露, 会为他们带来极大的生活影响, 这也就为什么一定要加强网络安全的使用。

一、网络安全的概念

网络安全就是指在信息网络的硬件以及软件管理过程中, 能够不受到外界的影响和其他措施的攻击, 可以使得计算机信息系统能够正常的运行。同时, 保障电脑上的信息也不会得到相应的泄露。随着互联网技术的不断发展, 人与人之间能够完全的借助互联网去突破时间和时空的一些限制, 加强了人们之间的交流和沟通, 而

且为人们带来极大的便利, 用户可以足不出户就完成自己想要完成的事情, 从而提高了他们的幸福指数以及满意度。但是在当前信息传递的速度也得到了飞速的发展, 用户可以通过手机就能够全面的了解当前全国各地所发生的重大事件, 改变了过去信息封锁的状态。然而, 网络时代下, 人们除了获取信息的速度提高之外, 人们所获得信息的范围也不断的增加, 通过搜索引擎可以获取更多的答案。网络技术的发展以不同的方式改变了人们的生活。因此, 人们在获得信息的过程中, 也会不经意间将个人信息发布在网上。同时, 如果人们点开一些网页或者是广告, 这些广告会自动的识别个人信息和位置。所以这就容易导致个人和企业的信息遭到泄露, 从而对个人和企业产生巨大的影响, 以及财产的损失。所以要更好的保障人们使用网络的安全性, 就需要提高安全意识以及信息网络安全。

二、推进网络安全工作的意义

2.1 维持网络秩序的稳定与安全

人们使用互联网, 主要就是为了获取各种的信息, 所以人们也将个人的信息反馈到互联网上进行传递和分享, 通过互联网能够了解到自己知道的内容, 而且也增长了用户的见识。但是互联网的建设和发展并不是一直都是安全的, 互联网它的运营是由维修工人来完成的, 但由于互联网是一个新的产物, 因此, 在发展的过程中存在着一系列的问题, 就需要不断的去发现问题, 解决问题。网络安全工作也是需要时时的维护, 而

且还要定期的对系统进行更新，这样才能够维护整个互联网的稳定性，解决这些互联网的漏洞，是为了更好的不被不法分子窃取信息以及传播病毒。因此，开展网络安全工作过程中，一定要保证互联网的安全和稳定，这样才能够提高个人和企业对于互联网的信任，能够放心的使用互联网。而技术人员只有不断的对互联网进行更新以及填补互联网中的漏洞才可以更好地发挥互联网的作用，使得互联网为人们带来更多的便利。

2.2 提升用户对网络安全的认知

在开展和推进网络安全工作过程中，一定要通过网络的宣传渠道来提醒人们对于安全意识的重视力度。在当前我们可以发现，有许多不法分子，他们利用互联网技术来骗取钱财。同时，许多不同年龄段的人受到钱财的欺骗，像有些用户被骗子们的三言两语就骗走了几百万，主要原因就是因为人们缺乏对于个人隐私的重视以及对于信息安全的了解。所以为了更好的提高用户对于网络安全的认知，就需要相关人员可以加大宣传以及科普，能够让人们了解互联网在传播过程中的一些规律，并且要让他们提高相应的法律意识，在遇到不法分子通过各种传销或者是渠道来进行骗取钱财时，要及时的报警，并且在遵守互联网相应的法律法规时，还要规定好自己的行为举止，不要利用网络去做一些违法乱纪的事。

2.3 维系社会安定，保障国民经济稳定

随着互联网技术的深入发展，互联网在承载海量的信息资源过程中，也改变了各行各业的经营状态。一方面，个人和企业获取信息过程中，要与互联网进行连接，因为企业要想获得一些有用的信息，就需要将企业的消息传递出才可以获得其它的消息。另一方面，个人和企业的财产信息也处在互联网中，所以为了更好的保障信息的安全，就要切实的保障个人和企业的安全，能够不受到损害。所以从上午我们能够了解到网络安全的重要性以及它可以更好的稳定社会推动社会的和谐发展。

三、网络安全面临的威胁

在当前互联网以及大数据技术的不断发展，使得人们在生活和工作过程中都带来了巨大的便利，但是信息的传播速度较快，人们越来越离不开网络时代。在进行使用网络过程中会需要人们登录个人信息，这时，由于网络技术还是存在一定的问题，以及大数据技术的不完善，这就使得网络技术的发展对于人们和企业的隐私安全造成了一定的隐患。

3.1 个人隐私泄露

在当前处于大数据时代背景下，人们能够通过信息平台进行信息的交换，在这个过程中，人们不可避免的会在平台上发布自己的信息，而且现在各平台网站都需要个人用手机号或者是身份证号进行注册，而在这样的操作过程中，用户的银行卡和身份证以及联系地址就会遭到相应的泄露，从而严重影响着用户的隐私，所以给

用户带来了重大的财产安全问题。信息时代背景下，网络的安全是一个非常普遍的现象。但是，在未来，互联网和大数据的发展过程中，就要集中处理个人隐私遭到泄露的情况，通过提高互联网技术以及填补互联网漏洞，并且技术人员要积极的进行创新，完善大数据来增强网络的安全，从而减少用户隐私泄露的情况。

3.2 大数据技术的安全风险

经过研究和调查可以得知，在人们日常生活和工作中，人们对大数据技术的应用频率也是相对较高的，大数据能够随时记录人们的阅读、购物和出行习惯，这样能够有效减少了人们大量选择的时间，极大方便了人们的日常生活和工作。此外，在企业具体实践发展的过程中，大数据技术也能够有效帮助企业完成数据筛选、分析和储存等方面的需求，能够便于企业基于算法的基础上，对各个结果进行回馈，从而更好的掌握市场动态和客户群体的喜好，从而出符合市场需求的产品和服务，这也会对后期各项工作的开展有着较为重要的推动和促进作用。但是由于受各种内部因素和外部因素的影响，大数据技术具体应用和发展是由于其内部整体结构是相对简单的，经常会遭受黑客的清奇攻破，这样会使内部储存的信息泄露，不利于各个主流储存方式的提高，方式的提高反而会在乎具体展示，频繁出现各种各样的难题。对此，在今后我国大数据技术具体应用和发展是则应该不断加强对个人信息收集工作的重视力度，从而有效降低用户信息使用的风险。

3.3 智能终端的信息安全威胁

进入 21 世纪以来，随着我国 PC 端信息安全防护体系的不断完善，信息时代下移动端也呈现快速发展的趋势，信息传递重心逐渐由 PC 端转为移动端。和移动端和 PC 端相比较而言，移动端的安全防护体系是相对较低的，终端在后期具体应用和发展时，经常会出现信息数据泄露的，终端内部储存的信息、照片、视频等数据经常会出现泄露风险^[1]。因此，应该不断加强对移动端信息安全防护工作的重视力度。

3.4 产业数字化带来的风险

产业数字化主要就是指数据及数字技术在实体经济生产过程中的广泛应用，而随着产业数字化的出现，它使得信息变得更加透明，从而容易导致他人窃取机密。产业数字化主要就是以数据为关键要素，对产业链的上下游提供数字化的服务。然而，在当前信息时代快速发展的背景下，一些不法分子容易盗取这些关键的数据，从而为企业带来巨大的经济损失。

四、信息时代下网络安全防护策略

在信息时代背景下，网络安全的防护工作需要各部门共同努力，首先，从国家层面来讲，要加大立法以及完善相应的法律法规，从政府层面来讲，一定要加强相应的管控措施以及监督措施，能够严格的去规范网络的安全以及使用，定期对网站进行相应的抽查。从互联网

企业来讲,一定要提高道德修养和责任心,能够更好地为社会做出贡献,防止为了经济效益而贩卖他人的个人信息。同时,个人也要加大安全意识,能够提高自己的防范措施,再发现信息泄漏时,首先要及时的寻求警察的帮助以及关闭自己在网络上所登录的信息。

4.1 建立健全相关法规

随着当前互联网用户的不断增加,互联网有关的企业也在扩张,同时,网络时代的发展对推动社会的进步有了重要的支撑,对于人们的生活也产生了一定的影响,个人信息,与互联网之间的联系,每天都在发生,所以,互联网企业在获取这些信息使难度较低,这就导致一些不良企业为了获得更多的经济效益从出卖客户的个人信息而在当前个人信息出现诈骗的事件也层出不穷。因此,国家一定要建立健全相应的法律法规。但目前来看,我国出台的一些法律法规对于危害他人信息安全的规则还是不够的,明确以及法律不健全,并且,法律在完善的过程中较慢,而网络时代,信息更新速度较快,所以这就需要国家能够在今后可以深入的了解网络会出现的安全事故,以及信息安全问题能够针对这些所出现的问题加强管理并对未来可能会出现的一些危害网络安全的行为进行相应的预防和规范,这也就需要各级部门能够提高自己的责任心,可以加强执法力度,从而,真正的保障网络安全以及提高用户和企业的信息安全。

4.2 技术完善

人们在利用信息技术进行信息的获取过程中,也需要借助网络的平台,这样才能够使得信息进行相应的传递,但是网络平台,它分布在不同的时间中,从而能够将人们联系在一起,实现了无障碍的交流,然而,在传输信息的过程中,为人们带来了极大的便利。然而,在共享网络平台时,就会造成信息在传递的过程中遭到泄露,其中会包括用户的身份,账户密码和联系方式以及家庭情况等,从而引发了信息安全问题^[2]。并且,在当前互联网技术还存在着一定的不成熟现象,而大数据技术也会有一些漏洞,所以,在信息传递过程中,一些黑客或者是不法分子就会利用技术手段来找到这些漏洞,从而窃取用户的个人隐私获取牟利,所以,在未来发展过程中,需要加强互联网技术的运用。

4.2.1 加固网络节点,保障数据安全

加固网络节点,能够更好地保障数据的安全。信息传递和交互,在互联网过程中的每一个节点都要进行相应的防护,而且还要加强,对服务器进行加固,主要目的是为了能够保证信息在运输过程中不会出现问题,同时,大数据,长期的传送,使得网络的各个节点,也遭到了一定的破坏,因此就需要技术人员能够及时的跟进每一个节点,进行相应的,改造,从而提升整个节点的处理能力,保护信息安全的情况下能够使得,这些数据不被窃取,从而还可以提高数据的传输效率和速度。

4.2.2 革新防火墙技术加强防护信息数据的传递

在对这些虚拟数据进行传递的过程中,需要在网络中设置一个防火墙,而该防火墙用来阻断那些网络中的不良信息和有病毒的文件,并且防火墙的设置,他也能够减少互联网本身所存在的一些弊端。在计算机发生攻击时能够迅速的使用保护按钮,防止不法分子窃取计算机信息内容,并且,在当前随着技术的不断发展,新的防火墙技术也得到了相应的使用,它能够第一时间识别出病毒和外来的侵入,精准的对这些网站进行分析,从而避免黑客的攻击^[3]。

4.2.3 建立额外的云备份数据

用户在使用互联网过程中,一定要建立额外的云备份数据,他也是在信息时代下所出现的一个新的工具,能够通过检查以及定期的数据备份存储在云端中,能够与手机进行直接的连接,而该数据被不法分子通过病毒软件侵害之后,这些系统就会发出警报,如果用户采取了一些措施,无法得到挽救时,该信息就能够通过云端传输到用户手机上,并且他能够强制的停止不良程序,对于计算机网络的侵害而云备份数据,也能够增强本身对于信息的保护,防止信息遗失。

4.3 用户要加强个人信息保护意识

信息时代下,一定要加强个人信息的保护意识,除了依靠外部的法律保障外,用户也要加强个人信息保护的意识,在目前来看,许多信息平台,他们的内容非常多,人们在获取这些内容时,容易上当受骗,也容易被迷惑眼睛,所以,在面对信息获取的时候,一定要擦亮自己的眼睛,对一些非法的网站要有鉴别的意识,能够懂得哪些网站不随意输入个人信息,并且也要减少自己的好奇心,尽量不去点开危险广告,如果一旦点开,系统会自动的识别该用户的个人隐私信息,从而遭到了泄露。而且还需要在自己的电脑上安装一些杀毒软件,定期的进行信息的清理,对于重要信息,可以建立一个安全所以及防护密码,如果一旦系统遭到了黑客的袭击或者是泄露,咋这些个人信息就会自动销毁,但是他是先把信息传递到用户的手机云管家里面,再把电脑上的个人信息自动的清除,而用户定期的利用杀毒软件对这些病毒进行查杀,可以很好的预防信息的泄露。并且,用户在每一次输入完账号后不要忘记住密码,这样在下次登录时,就需要从新输入密码才可以。用户养成一个良好的上网习惯,就可以最大程度的有效规避在上网中会遇到的网络风险^[4]。

4.4 产业数字化安全应对策略

伴随着产业数字化新技术新场景的出现,企业在经营发展过程中,一定要提高容量的安全性。而 MEC 边缘云已然成为 5G 新基建的风向标,以 MEC 边缘云为触点,实现“规、建、维、研、营”一体化。自研核心平台,增强网络联接的控制与管理,实现从“产品推送”到“营销支撑”的商业闭环。同时,企业也要将云计算,大数据等智能技术运用到企业的业务中从而加快企业产业数

字化的发展。IPv4 最大的问题在于网络地址资源不足，严重制约了互联网的应用和发展。因此，在未来发展过程中，就要加强安全管理，提升从业人员的素质同时，也要加大对 IPV4 安全威胁和防护技术的研发，将 IPV4 向 IPV6 转变。

五、结束语

综上所述，我们能够了解到信息技术的发展，除了给人们带来极大的便利，也使得人们的个人信息和隐私遭到了相应的泄露。所以无论是个人的隐私还是企业的一些数据都是非常重要的，在进行发展过程中，就需要通过外部的防御和内部的管理，从而提高网络的安全性。并且在加强外部管理过程中，一定要建立一个安全的法律环境，通过加强立法来对那些危害网络安全的一些行为进行相应的惩罚，使得他们能够严格的遵守网络安全

秩序和规定，并且内部系统也要提高个人以及企业的一些操作，这样从根本上提高信息安全的意识。

参考文献：

[1] 谢生光. 关于信息时代背景下的电子信息安全管理分析 [J]. 电脑迷, 2017(07):54.

[2] 王浩轩. 信息时代背景下的电子信息安全管理分析 [J]. 数码世界, 2016(12):63-64.

[3] 顾建龙. 浅谈信息时代背景下的电子信息安全管理 [J]. 电子技术与软件工程, 2014(17):224-225

[4] 司明星, 李秋月. 信息时代下信息通信网络安全管理策略 [J]. 信息周刊, 2020(9):1.

作者简介: 呼博文(1984-), 男, 汉族, 河北, 本科, 学生, 主要研究方向安全中台规划、建设、应用等、5G 网络安全架构等。